METHOD AND APPARATUS FOR A TRUST PROCESSOR

Abstract

In an embodiment, an apparatus includes a cryptographic processor within a wireless device. The cryptographic processor includes at least one cryptographic unit. The cryptographic processor also includes a nonvolatile memory to store one or more microcode instructions, wherein at least one of the one or more microcode instructions is related to a sensitive operation. The cryptographic processor also includes a controller to control execution of the one or more microcode instructions by the at least one cryptographic unit, wherein the controller is to preclude execution of the sensitive operation if the apparatus is within an untrusted state.

"Express Mail" mailing label number: EV 370239793 US
Date of Deposit: March 31, 2004
This paper or fee is being deposited on the date indicated above with the United States Postal Service pursuant to 37 CFR 1.10, and is addressed to the Commissioner for Patents, Mail Stop Patent Application, P.O. Box 1450, Alexandria, VA 22313-1450.